CLAIMS

What is claimed is:

1. A method of determining network penetration, the method comprising the computer-implemented steps of:

representing a possible travel of a packet in a network based on topology data and on security policy data; and,

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing.

2. A method as recited in Claim 1, wherein the security policy data comprises one or more access control lists of one or more network devices in the network.

3. A method as recited in Claim 1, further comprising the step of receiving packet parameters.

4. A method as recited in Claim 3, wherein the packet parameters comprise an entry point where the packet enters the network.

5. A method as recited in Claim 3, wherein the packet parameters comprise a destination address.

6. A method as recited in Claim 1, wherein the topology data is received as input related to a user interface.

7. A method as recited in Claim 1, wherein the security policy data is based on access control lists associated with input received in a user interface.

8. A method as recited in Claim 1, further comprising determining a maximum penetration point.

9. A method as recited in Claim 1, wherein the step of representing comprises accessing the security policy data and the topology data related to a network device for which it has been determined that the packet could reach.

10. A method as recited in Claim 1, wherein the step of representing comprises determining whether ingress is allowed to a network device for which it has been determined that the inbound interface could be reached by the packet.

11. A method as recited in Claim 1, wherein the step of representing comprises determining whether there are any neighboring network devices to a network device for which it has been determined that the packet could reach.

12. A method as recited in Claim 1, wherein the step of representing comprises determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

13. A method as recited in Claim 12, wherein the step of representing comprises recursively applying the step of determining whether there are any outbound interfaces.

14. A method as recited in Claim 1, wherein the step of representing comprises:
checking an inbound access control list (ACL) of an interface of a network device comprising a simulated network entry point for the packet;
if the inbound access control list permits ingress of the packet, checking one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted;

for each of the one or more possible outbound interfaces on which the egress of the packet is permitted, repeating the checking steps with respect to each neighbor network device that is connected to each of the one or more possible outbound interfaces.

15. A method as recited in claim 1 further comprising receiving packet parameters specifying information corresponding to a plurality of packets.

16. A method as recited in claim 1 wherein the step of representing comprises:
at a network device that for which it is determined that the packet could reach, determining if a static routing table is present; and
if the static routing table is present, then
accessing the static routing table, and
determining an outbound interface through which egress is permitted based on the static routing table.

17. The method of claim 16, further comprising not permitting egress through an outbound interface permitted by the static routing table, but not permitted by an access control list associated with the security policy.

18. A method as recited in claim 1 wherein the step of representing comprises:
at a network device for which it is determined that the packet could reach, determining if a static routing table is present; and
if the static routing table is not present, then for each outbound interface, representing an egress by the packet as part of the representing of the travel of the packet.

19. A method as recited in claim 1, further comprises receiving packet parameters that support transmission control protocol flags.

20. A method as recited in claim 1, wherein the results comprise a graphical display of at least allowed paths of the packet.

21. A method as recited in claim 19, wherein the graphical display also includes at least a mapping of network devices and connections between the network devices.

22. A method of determining potential penetration of a packet into a network, the method comprising the computer-implemented steps of:
receiving network topology data;
receiving first information defining a packet flow comprising a source address;
receiving second information defining a first network device, comprising a network address and an ingress interface identifier for an ingress interface;
determining whether the ingress interface of the first network device allows the packet flow to enter the first network device, based on a first access control list associated with the ingress interface;
determining one or more egress interfaces of the first network device that allow egress of the packet flow, based on one or more second access control lists associated with the one or more egress interfaces;
based on the network topology data, determining one or more second network devices that are coupled to the one or more egress interfaces; and
recursively performing the determining steps for each of the one or more second network devices.

23. A method as recited in Claim 22, further comprising the steps of determining if a static routing table is present, and wherein the step of determining the one or more egress interfaces is performed based on the static routing table.

24. The method of claim 23, further comprising not permitting egress through an outbound interface permitted by the static routing table, but not permitted by the one or more access control lists.

25. A method of determining network penetration, the method comprising the computer-implemented steps of:

representing a travel of a packet in a network based on topology data and on security policy data including at least

defining a packet by at least specifying a source address, an entry port, and a destination port;

starting a loop for a current network device;

accessing access control list (ACL) data stored in an ACL database and the topology data stored in a topology database;

deciding whether an ingress interface of a current network device allows entry into the current network device,

if the entry is not permitted, then terminating the loop for the current network device,

if the entry is permitted continuing the loop;

determining if a static routing table is present,

if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and

if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces;

determining if there are any neighboring network devices,

if there are not any neighboring network devices, then an indication of the current network device is returned as a maximum penetration point as at least part of results of the step of representing, and the loop is terminated;

if there is a neighboring network device, then the loop continues

determining whether or not there are any remaining outbound interfaces for which results of a possible egress of the packet have not been determined,

if there are no more remaining outbound interfaces, then the loop is terminated,

if there are more remaining interfaces, then
the current network device is set to the neighboring network device to corresponding one of the remaining outbound interfaces, and
if the loop has not been terminated for the current network device, restarting the loop for the current network device.

26. A system for determining penetration into a network, the system comprising:
one or more processors;
a topology database storing topology information about the database;
an Access Control List (ACL) database storing ACL information related to the network;
a computer-readable medium carrying one or more sequences of instructions for displaying a penetration Graphical User Interface (GUI) including at least
input fields having at least
a topology information input field,
an ACL input field,
a source address input field for entering at least a source address of a packet,
an entry point entry field for entering at least a one entry point to the network for the packet, and
a destination input field for entering at least a destination address for the packet, and
output penetration information including at least a graphical output including at least a representation of
network devices of the network,
connections between the network device corresponding to the topology data,
at least one entry point to the network,
paths the packet is allowed to follow based on the topology data and the ACL data,
at least one maximum penetration point; and

a penetration module that

accesses the topology database,

accesses the ACL database,

receives input corresponding to the input fields, and

produces the output penetration information for display in the penetration GUI.

27. A system for determining network penetration, the system comprising:

one or more processors, and a computer-readable medium carrying one or more sequences of instructions for causing the one or more processors to carry out a method comprising the step of:

representing a possible travel of a packet in a network based on topology data and on security policy data; and,

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing.

28. A system as recited in Claim 26, wherein the security policy data comprises one or more access control lists stored on one or more network devices in the network.

29. A system as recited in Claim 26, the method further comprises the step of receiving packet parameters.

30. A system as recited in Claim 29, wherein the packet parameters comprise an entry point where the packet enters the network.

31. A system as recited in Claim 29, wherein the packet parameters comprise a destination address

32. A system as recited in Claim 27, wherein the topology data is based on input related to a user interface.

33. A system as recited in Claim 27, wherein the security policy data is based on access control lists associated with input related to a user interface.

34. A system as recited in Claim 27, wherein the method further comprises determining a maximum penetration point.

35. A system as recited in Claim 27, wherein the step of representing comprises accessing the security policy data and the topology data related to a network device for which it has been determined that the packet could be reach.

36. A system as recited in Claim 27, wherein the step of representing comprises determining whether ingress is allowed to a network device whose inbound interface for which it has been determined that the packet could be reach.

37. A system as recited in Claim 27, wherein the step of representing comprises determining whether there are any neighboring network devices to a network device for which it has been determined that the packet could reach.

38. A system as recited in Claim 27, wherein the step of representing comprises determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

39. A system as recited in Claim 38, wherein the step of representing comprises recursively applying the step of determining whether there are any outbound interfaces.

40. A system as recited in Claim 27, wherein the representing of the travel of the packet comprises:

checking an inbound access control list (ACL) of an interface of a network device comprising a simulated network entry point for the packet;

if the inbound access control list permits ingress of the packet, checking one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted;

for each of the one or more possible outbound interfaces on which the egress of the packet is permitted, repeating the checking steps with respect to each neighbor network device that is connected to each the one or more possible outbound interface.

41. A system as recited in claim 27 wherein the packet parameters specify information corresponding to a plurality of packets.

42. A system as recited in claim 27 wherein the step of representing comprises:

at a network device being represented as having been reached by the packet, determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress is permitted based on the static routing table.

43. The system of claim 42, the method further comprising not permitting egress through an outbound interface permitted by the static routing table, but not permitted by an access control list associated with the security policy.

44. A system as recited in claim 27, wherein the step of representing comprises:

at a network device for which it is determined that the packet could reach, determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface, representing an egress by the packet as part of the representing of the travel of the packet.

45. A system as recited in claim 27, further comprises receiving packet parameters that support transmission control protocol flags.

46. A system as recited in claim 27, wherein the results comprise a graphical display of at least allowed paths of the packet.

47. A system as recited in claim 27, wherein the graphical display also includes at least a mapping of network devices and connections between the network devices.

48. A system as recited in Claim 27, wherein the step of representing comprises:
defining a packet flow by at least specifying a source address, a source port, and a destination port;
starting a loop for a current network device;
accessing the ACL data stored in an ACL database and the topology data stored in a topology database;
deciding whether an ingress interface of a current network device allows entry into the current network device,
if the entry is not permitted, then terminating a loop for the current network device,
if the entry is permitted continuing the loop;
determining if a static routing table is present,
if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and
if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces;
determining if there are any neighboring network devices,
if there are not any neighboring network devices, then
an indication of the current network device is returned, as results of the step of representing, as a maximum penetration point, and
the loop is terminated, and
if there is a neighboring network device, then the loop continues;

determining whether or not there are any remaining outbound interfaces that the packet has not reached,

if there are no more remaining outbound interfaces, then the loop is terminated, and

if there are more remaining interfaces, then

the current network device is set to the neighboring network device corresponding one of the remaining outbound interfaces; and

if the loop has not been terminated for the current network device, restarting the loop for the current network device.

49. A computer-readable medium carrying one or more sequences of instructions for determining network penetration, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the step of:

representing a possible travel of a packet in a network based on topology data and on security policy data; and,

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing.

50. A computer readable medium as recited in Claim 49, wherein the security policy data comprises one or more access control lists of one or more network devices in the network.

51. A computer readable medium as recited in Claim 49, wherein the instructions further comprise the step of receiving packet parameters.

52. A computer readable medium as recited in Claim 51, wherein the packet parameters comprise an entry point where the packet enters the network.

53. A computer readable medium as recited in Claim 51, wherein the packet parameters comprise a destination address.

54. A computer readable medium as recited in Claim 51, wherein the instructions further comprise the step of reading topology information from a topology database.

55. A computer readable medium as recited in Claim 49, wherein the topology data is based on input related to a user interface.

56. A computer readable medium as recited in Claim 49, wherein the security policy data is based on access control lists associated with input related to a user interface.

57. A computer readable medium as recited in Claim 49, wherein the instructions further comprise the step of determining a maximum penetration point.

58. A computer readable medium as recited in Claim 49, wherein the step of representing comprises accessing the security policy data and the topology data related to a network device for which it has been determined that the packet could reach.

59. A computer readable medium as recited in Claim 49, wherein the step of representing comprises determining whether ingress is allowed to a network device whose inbound interface for which it has been determined that the packet could be reach.

60. A computer readable medium as recited in Claim 49, wherein the step of representing comprises determining whether there are any neighboring network devices to a network device for which it has been determined that the packet could be reach.

61. A computer readable medium as recited in Claim 49, wherein the step of representing comprises determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

62. A computer readable medium as recited in Claim 49, wherein the step of representing comprises recursively applying the step of determining whether there are any outbound interfaces.

63. A computer readable medium as recited in Claim 49, wherein the representing comprises:

checking an inbound access control list (ACL) of an interface of a network device comprising a simulated network entry point for the packet;

if the ingress is permitted, checking the outbound ACLs for each outbound interface of the network device at which the packet has arrived to determine possible outbound interfaces on which egress of the packet is permitted;

for each of the possible outbound interfaces on which the egress of the packet is permitted, move the packet to a connected network device that corresponds to the network interface and repeat the step of checking an inbound egress and the step of if the ingress is permitted checking the outbound ACLs.

64. A computer readable medium as recited in Claim 49, wherein the instructions further comprise the step of packet parameters specifying information corresponding to a plurality of packets.

65. A computer readable medium as recited in Claim 49, wherein the step of representing comprises:

at a network device reached, determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress is permitted based on the static routing table.

66. The computer readable medium of claim 65, the method further comprising not permitting egress through an outbound interface permitted by the static routing table, but not permitted by an access control list associated with the security policy.

67. A computer readable medium as recited in Claim 51, wherein the step representing comprises:
at a network device reached, determining if a static routing table is present; and
if the static routing table is not present, then for each outbound interface, representing an egress by the packet as part of the representing of the travel of the packet.

68. A computer readable medium as recited in Claim 51, wherein the instructions further comprise the step of receiving packet parameters that support transmission control protocol flags.

69. A computer readable medium as recited in Claim 51, wherein the results comprise a graphical display of at least allowed paths of the packet.

70. A computer readable medium as recited in Claim 69, wherein the graphical display also includes at least a mapping of network devices and connections between the network devices.

71. A computer readable medium as recited in Claim 51, wherein the step of representing comprises:
defining a packet flow by at least specifying a source address, a source port, and a destination port;
starting a loop for a current network device;
accessing the ACL data stored in an ACL database and the topology data stored in a topology database;
deciding whether an ingress interface of a current network device allows entry into the current network device,

if the entry is not permitted, then terminating a loop for the current network device,

if the entry is permitted continuing the loop;

determining if a static routing table is present,

if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and

if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces;

determining if there are any neighboring network devices,

if there are not any neighboring network devices, then an indication of the current network device is returned as results of the step of simulation as a maximum penetration point, and the loop is terminated, and

if there is a neighboring network device, then the loop continues;

determining whether or not there are any remaining outbound interfaces that the packet has not reached,

if there are no more remaining outbound interfaces, then the loop is terminated, and

if there are more remaining interfaces, then

the current network device is set to the neighboring network device corresponding one of the remaining outbound interfaces; and

if the loop has not been terminated for the current network device, restarting the loop for the current network device; and

the method further comprising the step of:

displaying the results of the simulating by at least displaying

an allowed packet path, if found, and

the maximum penetration point.

72. A system for determining network penetration comprising:

means for representing a possible travel of a packet in a network based on topology data and on security policy data; and,

means for providing an output that specifies a possible penetration of the packet into the network, based on the step of representing.